vocality
Efficient Networks

Configuring SSH on Vocality units

Application Note AN309
Revision v1.3
September 2015

AN309 Configuring SSH

SSH requires the Security software (RTUSEC) and a Feature Key on all products.

1 Overview

This Application Note explains how you can configure an SSH server on Vocality units (with software VOS06_03.01C or later), once you have set up the menus below the **SSH Server menu** to permit either a password or pre-shared key form of SSH. (Refer to the **Menus** appendix for details of all the parameters that can be set.)

Overview: SSH Server

Secure Shell (SSH) is a network protocol, which allows data exchange using a secure channel between two network devices. SSH is an alternative to remote shells which send information, in particular passwords, in plain text, posing a security risk. SSH encryption offers confidentiality and data integrity over unsecured networks.

The SSH server is present in all nodes that support IP – so on a chassis based system (V150 or V200), there will be a separate SSH client on each slot that supports IP.

Vocality does not provide an SSH client. Commercial and freeware SSH clients (such as PuTTY) are available for several platforms. Any client that supports the standard SSH-2 protocols and provides a subset of common cryptography, message digest, key exchange and authentication mechanisms with the server is suitable.

2 Access table entry

The IP address, or network, of units permitted to access your unit needs to be specified in the **IP > Access Table**, shown in Figure 1 .

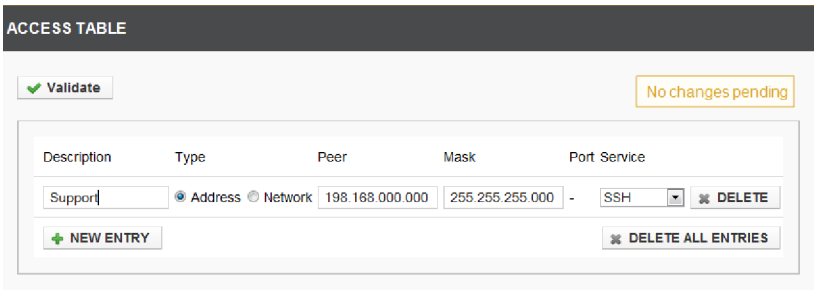

Figure 1 IP > Access Table menu

3 Operation

An SSH client needs to be used once the unit has been configured.

In key authentication mode, the private key generated by the key generator needs to be entered into the appropriate section of the client. (A private key generator is a separate third party software program, for instance PuTTYgen.) In PuTTy this is done by uploading the key file, in the window shown in Figure 2 .

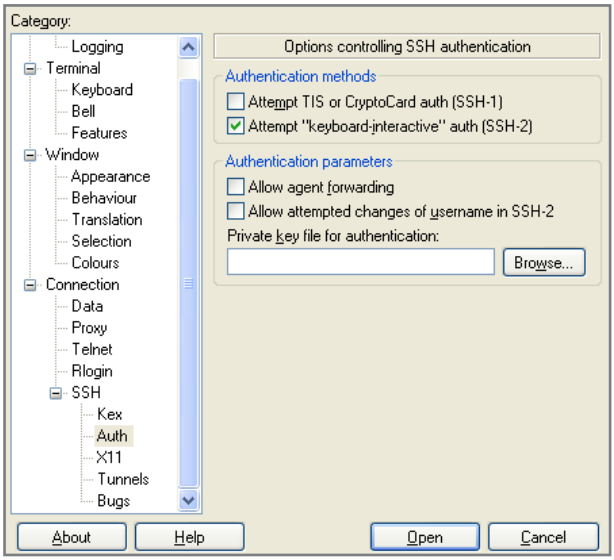

Figure 2 PuTTy configuration

The SSH client then needs to be targeted at your unit. If asked for a username or login name, you should use the node name of the unit. In password authentication mode, the node name of the unit and passwords must be used. For more information about the interaction of SSH user names and passwords with user access controls configured for the unit see section 5 Logging in from SSH.

4 Diagnostics

Two user-level diagnostics commands may be of use.

The **`ssh info`** command reports information about any connected clients (client address, crypto and HMAC algorithms used). For example, with a single client connected:

```
Dbg> ssh info
SessionID: 4097
Client address: 192.168.000.021
InCipher: aes256-ctr
InMAC: hmac-sha1
OutCipher: aes256-ctr
OutMAC: hmac-sha1
```

The session ID supplied may be used to force the disconnection of this client. The **`ssh disconnect`** *session ID* command can be used for this. You will need to specify the Session ID of the client to disconnect. For example:

```
Dbg> ssh disconnect 4097
Closing SSH session 4097...
Complete
```

5 Logging in from SSH

SSH expects a username and a password.

Note: You will only be permitted SSH access if IP > Access Table entries have been configured to allow SSH client access.

5.1 SSH password mode

The account name and password supplied across SSH are validated: the unit will support the full set of configured passwords.

Once this validation has happened, the unit presents any configured welcome message and then re-prompts for the password.

Logout from the Vocality unit will leave the SSH session active – so you can login again with the same or different password from that used to open the SSH session.

Note: For some users, such as the US DoD, it is important that a customised welcome message is presented before the login attempt happens. This method ensures that this happens, at the slight cost of entering the account/password twice.

If no accounts are configured (or accounts are not enabled) then SSH will accept the unit's node name as the login name and any password will be accepted.

5.2 SSH key mode

When the SSH server is configured for key authentication, the public key should be configured in the **SSH > Key & Authentication menu**. This public key must be the public key component from the private key on the SSH client.

The login name used for SSH authentication is always the unit's node name.

If accounts are enabled, then after SSH key negotiation has completed you will be presented with a login prompt. At this point you will need to use configured account details to access the menus.

If accounts are not enabled, then after SSH key negotiation has completed you will be able to access the menus straightaway.

6 About Application Notes

Application Notes are intended as a supplement to, rather than a substitute for, your User Manual. Should you have queries which are not answered by our current documentation, your local Vocality support team would be happy to hear from you.
E-mail **support@vocality.com**.

A Menus

A.1 SSH Server menu

The feature is only available in the secure variant of software.

The SSH Server menu allows generation of the host key, configuration of the user authentication mechanism (password or pre-shared key-based), selection of the crypto algorithms available and selection of the HMAC algorithms available.

A.1.1 SSH > Key & Authentication menu

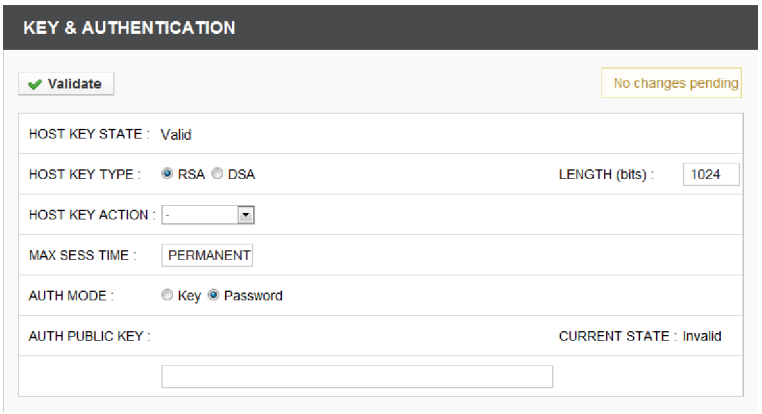
KEY & AUTHENTICATION
Validate
No changes pending
HOST KEY STATE : Valid
HOST KEY TYPE : RSA DSA
LENGTH (bits) : 1024
HOST KEY ACTION : -
MAX SESS TIME : PERMANENT
AUTH MODE : Key Password
AUTH PUBLIC KEY :
CURRENT STATE : Invalid

Figure 3 SSH > Key & Authentication menu - Password mode

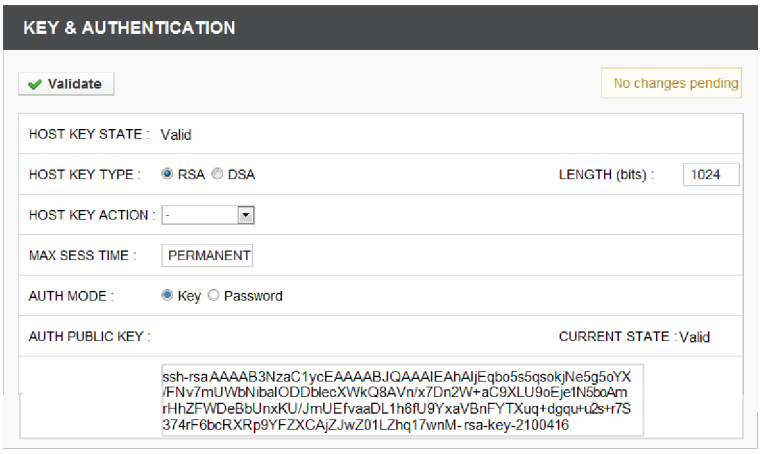

Figure 4 SSH > Key & Authentication menu - Key mode

The SSH Key & Authentication menu presents configuration parameters and controls for host keys used during asymmetric cryptography, session timeouts, and session authentication settings. Please refer to your User Manual for information about how user passwords are used with SSH.

Parameter	Range	Default	Use
Host Key Control			
HOST KEY STATE	Valid/Invalid	-	Read-only. Reports the state of the current host key. There must be a valid host key present for the SSH to work.
HOST KEY TYPE	RSA/DSA	RSA	Type of host key to use. (Note: The host key will be regenerated when this field is changed.)
LENGTH (bits)	512-40962048	1024	Length of key to generate in bits. This must be a multiple of 128 bits – will be rounded down to nearest multiple on entry if incorrect. (Note: The host key will be regenerated when this field is changed.)
HOST KEY ACTION	- / Regenerate / Zeroize	-	Regenerate the host key or zero it (Note: When the key is regenerated or zeroed, only subsequent SSH connections made will be affected – existing connections will use the host key that was present when they connected.)
Session Control			
MAX SESS TIME	10-1440 or PERMANENT	PERMANENT	Maximum session time in minutes. Use PERMANENT for unlimited session time
Authentication Control			
AUTH MODE	Password/Key	Key	Authentication mode required
AUTH PUBLIC KEY	String entry	-	The public key to use for key authentication mode
CURRENT STATE	Valid/Invalid	-	Read-only. Reports the state of the current authentication key.

Table A-1 Parameters in the SSH > Key & Authentication menu

When configuration changes are saved, a new host key will be generated and stored if any of the following conditions occur:

- current host key is invalid;
- host key type has been changed;
- host key length has been changed;
- host key action is set to regenerate.

Host key generation can be a lengthy operation. A progress indicator shows elapsed time against an estimated worst case. For RSA keys longer than 1024-bits this process can take minutes, or even tens of minutes to complete. Please wait for the key generation and save mechanism to complete. You cannot interrupt the key generation mechanism. Unit configuration may be corrupted and lost if you switch power off before key generation is complete.

Note: On the first connection following key generation, or regeneration, there will be a warning. This indicates that the server host key has changed from a previously cached value.

If the client is attempting to authenticate the server, then the client will need to be updated with the server's host public key following any key regeneration.

A.1.2 SSH > Crypto menu

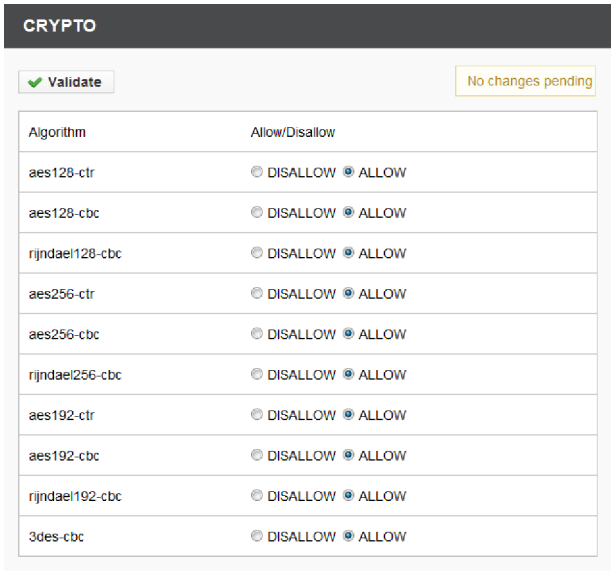

Figure 5 SSH > Crypto menu

The Crypto menu controls which symmetric cryptographic algorithms are advertised to the client during SSH protocol negotiation. By default all algorithms are allowed. This can be used to ensure a minimum strength of encryption is used. A row is presented for each crypto algorithm supported. Each can be set to ALLOW or DISALLOW.

A.1.3 SSH > HMAC menu

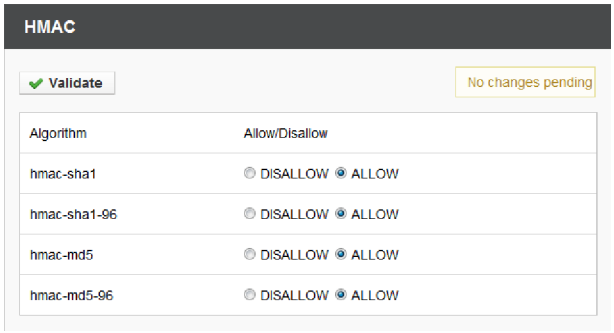

Figure 6 SSH > HMAC menu

The HMAC menu controls which message digest (hash-based message authentication code) algorithms are advertised to a client during SSH protocol negotiation. A row is presented for each mechanism supported, providing a parameter to ALLOW or DISALLOW each option. By default all algorithms are allowed to provide maximum interoperability.